Analysis of Resilience in Virtual Networks

İşil Burcu Barla¹², Dominic A. Schupke¹, Georg Carle²
¹ Nokia Siemens Networks, NSN Research, Munich, Germany
² Munich University of Technology, Munich, Germany

EuroView’11, Würzburg, Germany
August 1, 2011

Agenda

• Motivation
• Network virtualization model
• Failure types
• Comparison of resilience at different layers
  – Resource consumption
  – Service level resilience adaptability
  – Network setup and operation complexity
• Conclusion
• Q&A
Motivation

Resilience in Virtual Networks:

- Shared substrate resources
  - Enhanced efficiency
    - Increased effect of physical failures: many networks and services affected simultaneously

- Abstraction of the network
  - Increased flexibility and overall view possibility
    - More complex resilience design

- Different layers face different opportunities and challenges

Comparative analysis ➔ Optimal resilience design under different circumstances

Network virtualization model

VNO: Virtual Network Operator
VNet: Virtual Network

PIP: Physical Infrastructure Provider
Network virtualization model (cont’d)

Physical Infrastructure Provider (PIP):

- Owns the physical infrastructure
- Monitoring of the physical and virtual resources
  - Physical Resources (PR): Total access and control
  - Virtual Resources (VR): Knowledge of the usage and physical location
- Network utilization optimization: optimal VR allocation for all virtual networks (V Nets)
- Migration of VRs from one PR to another one
  - Overall optimization for all the V Nets residing on the physical network
  - Shutting down a part of the network (e.g. energy efficiency, maintenance purposes)

Network virtualization model (cont’d)

Virtual Network Operator (VNO):

- Owns and operates one or several V Nets
- VNet: virtual links and nodes
  - Requirements: node - CPU, memory, location, technology, …
  - link - bandwidth, delay, disjointness, …
  - Mapping to the network of one or more PIPs
- VNet request:
  - Advertisement of available virtual resources: PIPs → VNO
    → Overall view of the available resources!
  - Negotiation with various PIPs for establishing an optimal VNet
- Monitoring:
  - Buffer overflow, packet delay, …
Failure types

1) **Physical link/node failure:**
   - Transport link failure
   - Router/switch/server failure
   PIP → First one to detect the failure!

Resilience options:
1) Only PIP is responsible for resilience or VNO has no backup resource
2) Only VNO reacts due to the contract
3) Both can react
   - PIP: first one to detect the failure
   - Detected failure and recovery action taken signaled to VNO (also for Case 2)
   - Failure escalation with triggering
   - Hold-off timer

Failure types (cont’d)

2) **Virtual Machine (VM) failure:**
   2.1) Internal failure
       - VNO → The owner and controller of the VMs
       - PIP cannot (and shouldn’t) react

   2.2) Complete failure
       - No difference for VNO compared to physical failure

   2.3) Hypervisor failure
       - VNO cannot do anything

3) **Control plane failure:**
   - Topology Computation Engine
   - Network Management System
     } Data plane is still working
     Need to be extremely fast not seen
Comparison of resilience at different layers

• Failure types and cases to be considered:
  – Where both VNO and PIP are able to react
  – Where fast reaction is required
→ Physical node/link failures and complete VM failures

• Comparison metrics of having resilience at different layers:
  – Resource consumption
  – Service level resilience adaptability
  – Network setup and operation complexity

Comparison of resilience at different layers: Resource Consumption

**PIP:**

• Complete view of its network with…
  – its physical resources
    ▪ Available virtual resources on a physical resource
    ▪ Already leased resources and their properties
  – virtual resources residing on its network
    ▪ Their location
    ▪ Their properties

→ Optimizing the resource utilization regarding all VNets in the network
  – Migration of resources if necessary
  – Backup resource pools and shared protection
Comparison of resilience at different layers: Resource Consumption (cont’d)

**VNO:**
- Only limited view on the resources of a PIP
- No knowledge about the whole network structure of the PIP

However...
- Overall view over the available resources of all the PIPs
  ➔ Optimal combination of available resources from several PIPs for both primary and backup resources
  ➔ Sharing of the backup resources at the VNO level

Comparison of resilience at different layers: Service level resilience adaptability

**PIP:**
Limited: Should not influence service handling
  ➔ No optimization of resilience mechanisms possible depending on the actual services

**VNO:**
Comprehensive knowledge about the services and traffic characteristics in its VNets
  ➔ Optimization of the choice of backup resources and recovery actions accordingly
  ➔ Adaptation of the resilience level depending on the running services
Comparison of resilience at different layers: Network setup and operation complexity

**PIP:**
- Close to the origin for the considered failures
  ➔ More knowledge about the failure
  ➔ Fast reaction ability
- Multiple VNets share the same physical resource
  ➔ If the problem is fixed at the PIP layer, it is solved for all the affected VNets

**VNO:**
- No direct knowledge about the physical failures
  ➔ Need for signaling and coordination
- Due to one physical failure many VNets might be affected
  ➔ Need for separate reaction by each VNO
- Virtual resources for services should obey physical disjointness
  ➔ Need for disjointness information request
Conclusion

• Resource consumption
  – PIP: Complete knowledge of its network
    Optimization over all residing VNets
  – VNO: Overall view of the available resources of all PIPs

• Service level resilience adaptability
  – VNO: Optimization regarding the services

• Network setup and operation complexity
  – PIP: Simplicity regarding signaling and scalability

• Future work
  – Quantitative analysis of the results: Delay, resource consumption, cost, complexity
  – Design of appropriate resilience mechanisms

Q&A

Thank you for your attention!

Contact: isil.barla.ext@nsn.com